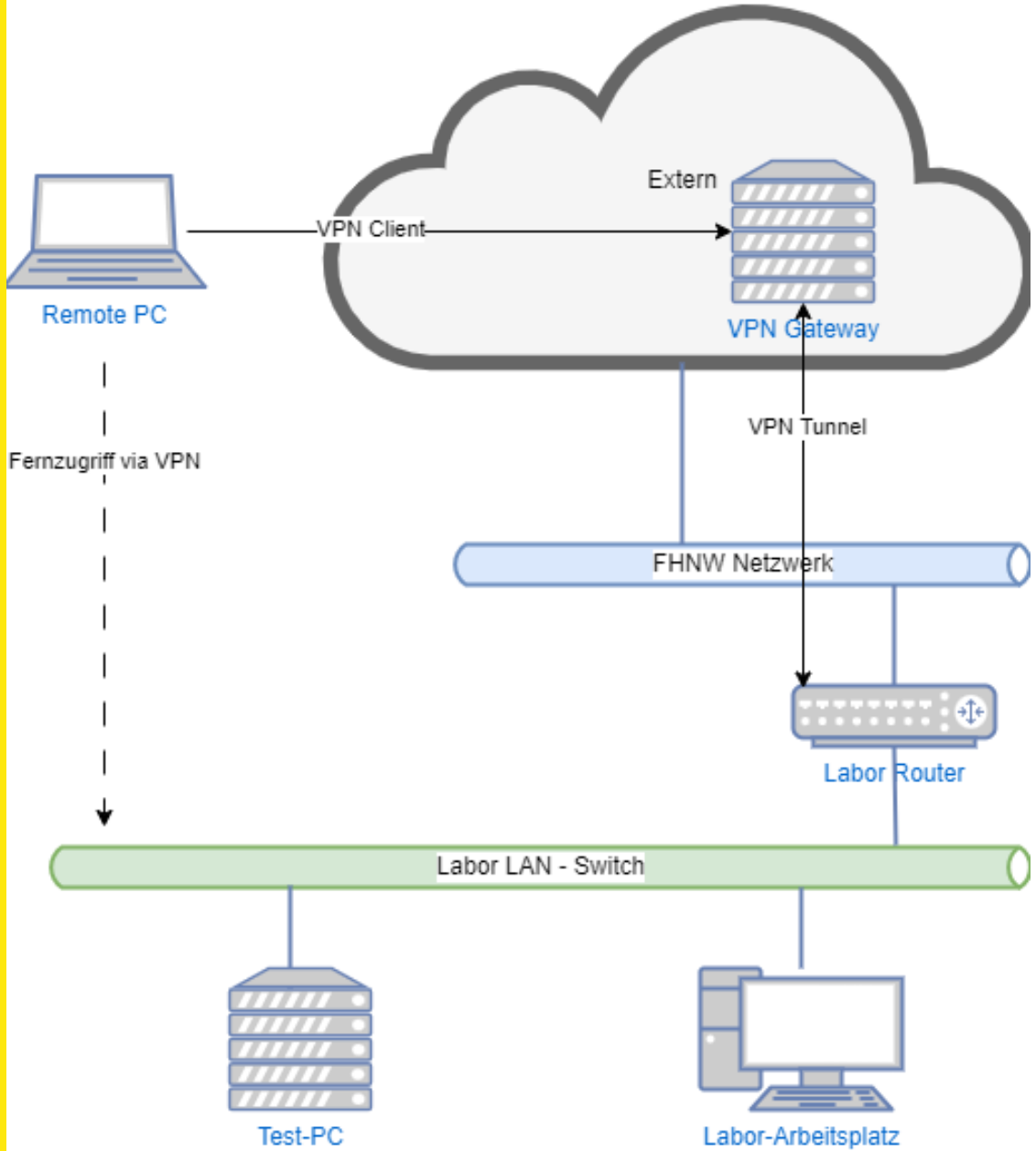
Fachhochschule Nordwestschweiz
Hochschule für Technik

Lab Connector – Fernzugriff auf Laboraufbauten

IMVS Tech Talk

Matthias Krebs

15. Mai 2024



Inhalt

1. Einführung und Anwendungsfälle
2. Frühere Lösungsansätze
3. Lab Connector

Einführung und Anwendungsfälle

Herausforderung

In Projekten, in denen mit Hardware gearbeitet wird, muss ggf. ein ganzes Labor-LAN ans Netzwerk angebunden werden.

Das kann aufwendig sein, sobald mehr als ein einzelnes Gerät involviert ist → Prozesse der Corporate IT

Ziel
- Universelle Lösung für die Verwendung in unterschiedlichen Projekten

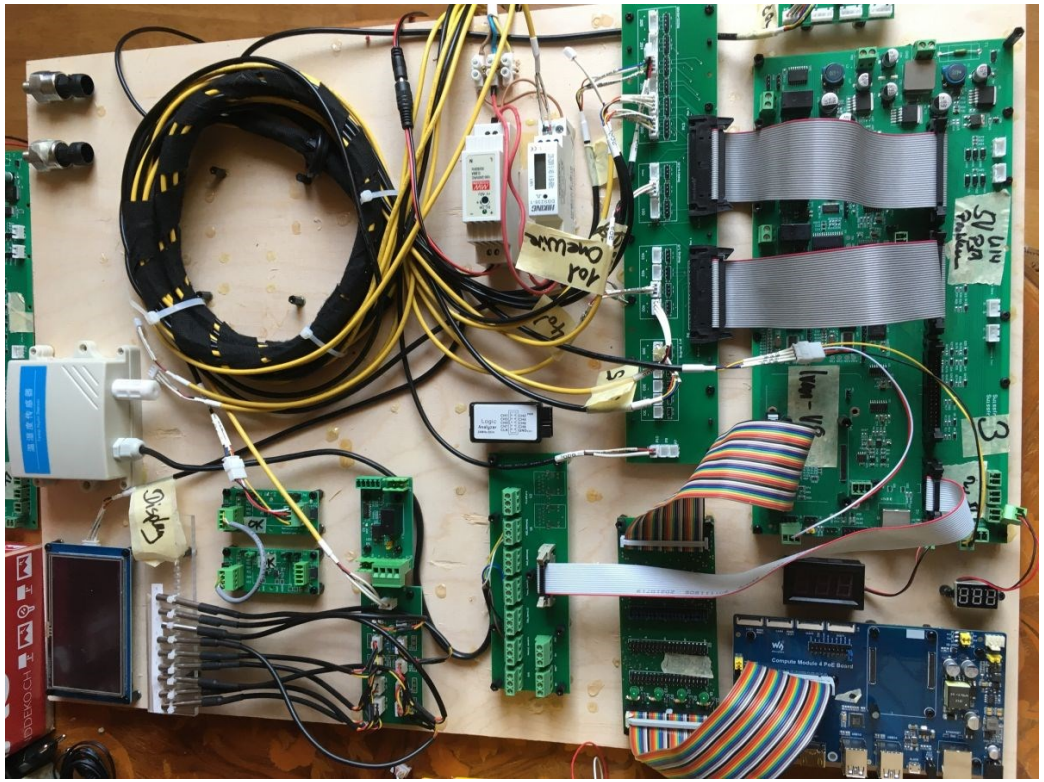
Anforderungen
- Niedrige Hardware-Kosten
- Flexibler Netzwerk-Zugriff, möglichst auch mit Fernzugriff
- Möglichst geringer administrativer Aufwand

Anwendungsfall 1 – Swissframe

Innosuisse-Projekt bis März 2024, IMVS

Badezimmer-Apparatur für Lüftung und Warmwassererzeugung, mit IoT-Anbindung

Benötigt ein Labor-LAN mit eigenem DHCP-Server zur Provisionierung der Embedded-Systeme (RPi Compute Module)



Vorläufer der Lab-Connector-Lösung

Anwendungsfall 2 – SmartGridready Testlabor

Vom BFE unterstütztes Projekt mit Verein SmartGridready, seit 2024, IA+IMVS

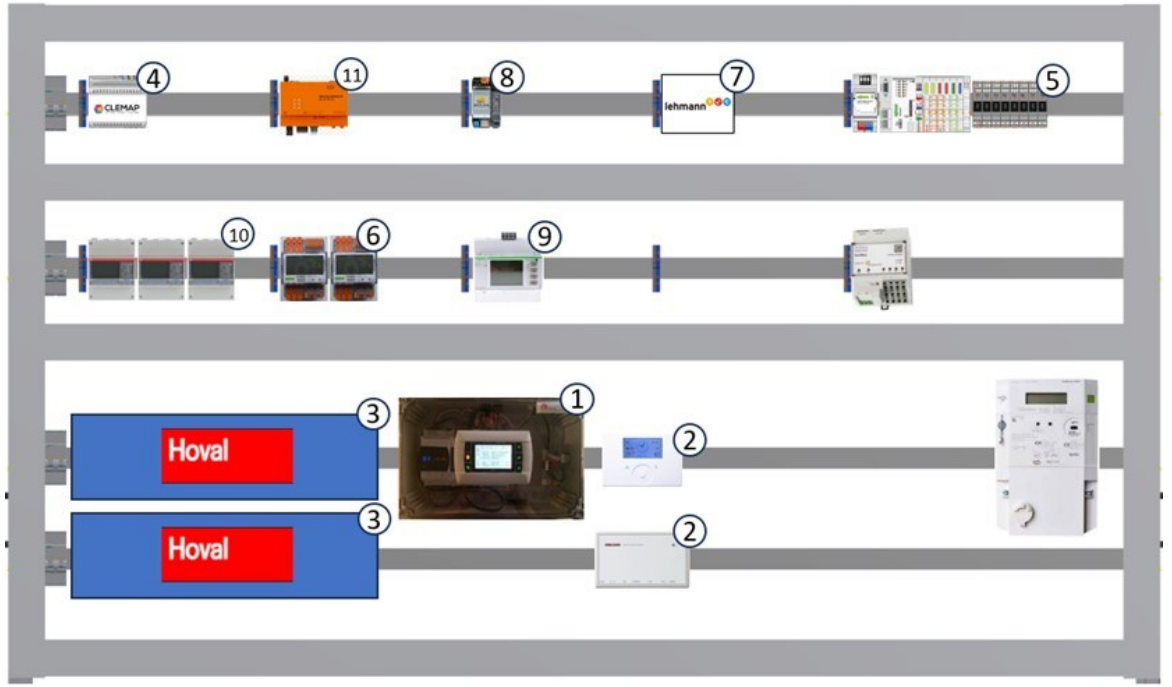
Offener Standard und Software-Stack zur Ansteuerung von Energiezählern, Wärmepumpen, Ladestationen usw.

Testlabor dient Herstellern zur Verifizierung der Kompatibilität mit SGr

Benötigt ein Labor-LAN mit Internetzugang und Fernzugriff, auch für Externe

Erste Anwendung der Lab-Connector-Lösung

www.smartgridready.ch



div. Energie-Messgeräte und -Steuerungen auf Alu-Gestell, meist mit LAN oder WLAN

Frühere Lösungsansätze

Labor-Router im EXP-Netz

Nach Freigabe durch die Corporate IT kann ein Router ins EXP-Netz (für Netzwerkgeräte ohne Authentifizierungsmöglichkeit) eingebunden werden.

Vorteile
- Keine Zugangsdaten nötig, nur MAC-Adresse muss freigeschaltet werden
- Fernzugriff via FHNW-VPN + NAT-Port-Forwarding möglich

Nachteile
- Abgesehen von einigen Standard-Ports müssen alle ein- und ausgehenden Verbindungen explizit freigeschaltet werden
- Kein transparenter Fernzugriff aufs Labor-LAN
- Auf ein Gebäude beschränkt

Labor-Router mit 802.1X

Wenn man einen Router verwendet, welcher 802.1X-Authentifizierung am WAN-Port unterstützt, kann er wie jedes persönliche Gerät ans FHNW-Client-Netzwerk angeschlossen werden.
Alternativ kann ein WLAN-Router als WLAN-Client konfiguriert und ins FHNW-WLAN eingebunden werden.

Vorteile
- Einfacher Zugriff auf FHNW-Netzwerk und Internet – keine Freischaltung nötig
- Funktioniert in jedem Gebäude

Nachteile
- Die meisten einfachen Router können kein 802.1X → nur mit Custom-Firmware machbar, z.B. **OpenWRT**
- Persönliche Zugangsdaten hinterlegt
- Zugriff auf interne FHNW-Ressourcen – evtl. nicht erwünscht
- Kein Fernzugriff möglich – auch nicht via FHNW VPN

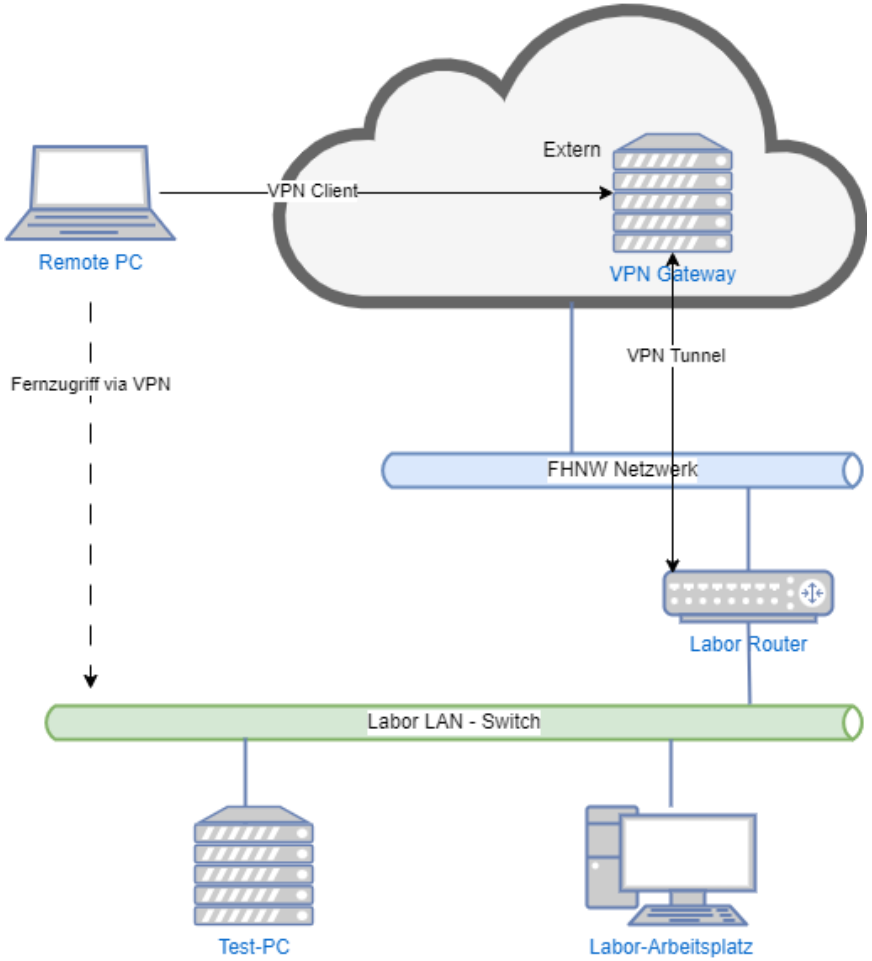
Lab Connector

Lab Connector – Überblick

Konzept

- Wireguard VPN
- VPN Gateway in Public Cloud
- Labor-Router baut VPN-Tunnel als Client auf → Internetzugang und Fernzugriff
- Remote-User verbinden sich mit VPN-Gateway → Zugriff auf Labor-LAN via VPN-Tunnel

- Mischung aus «Road Warrior» und «Site-to-Site»
- Router braucht nur ausgehende Verbindung – funktioniert auch hinter NAT

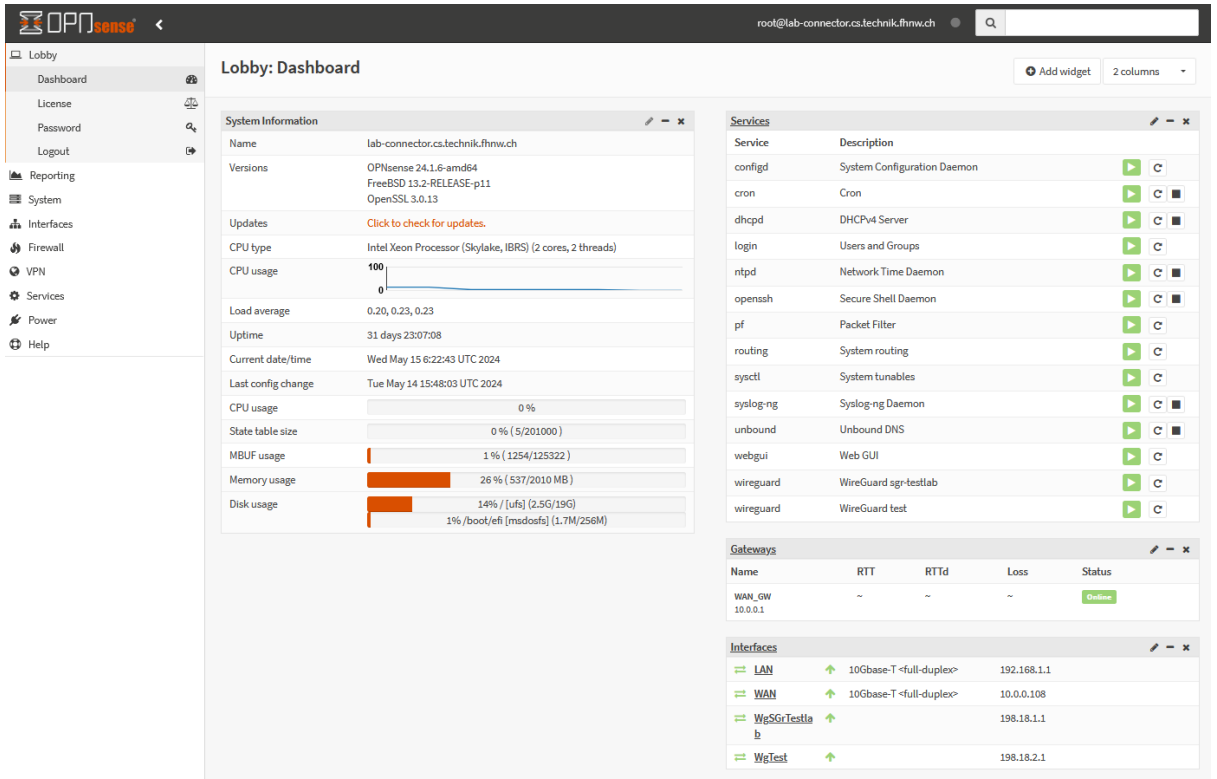


Lab Connector – VPN Gateway

OPNSense 24.1

- Open-source Router/Firewall
- Für PCs und Embedded-Systeme
- FreeBSD
- Wireguard VPN integriert

https://opnsense.org/



VPN Gateway in Cloud aufsetzen

Lab Connector VPN Gateway wird in einer Public Cloud (hier SwitchEngines) installiert.

Kein vordefiniertes Image für OPNSense in SwitchEngines vorhanden.

Lösung
Zuerst eine OPNSense VM lokal aufsetzen (z.B. VirtualBox) und als RAW-Image exportieren. Dieses kann in SwitchEngines importiert werden.

Konfigurationsanpassungen vor dem Export
- das Admin-Webinterface muss auch via WAN-Port erreichbar sein → Public IP kann in SwitchEngines nur einem Interface mit Route ins Internet zugewiesen werden
- HTTP_REFERER Check muss deaktiviert sein → wegen Public IP Mapping

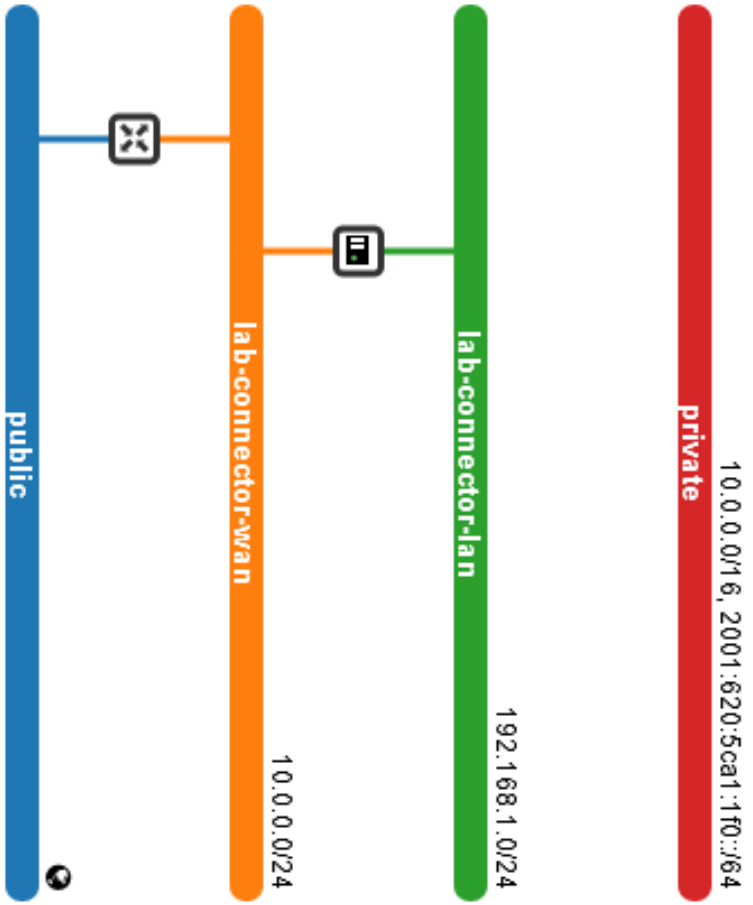
Cloud-Netzwerk für VPN Gateway

VPN Gateway wird wie ein herkömmlicher NAT-Router konfiguriert:

- 1 LAN (nicht benötigt, muss aber vorhanden sein)
- 1 WAN (Internet und externer Zugriff)
- N VPNs (nur intern auf GW)

1 Public IP Mapping
ext. Zugriff auf WAN-Adresse, Admin-Interface

Aktuell nur IPv4 – später evtl. auch IPv6

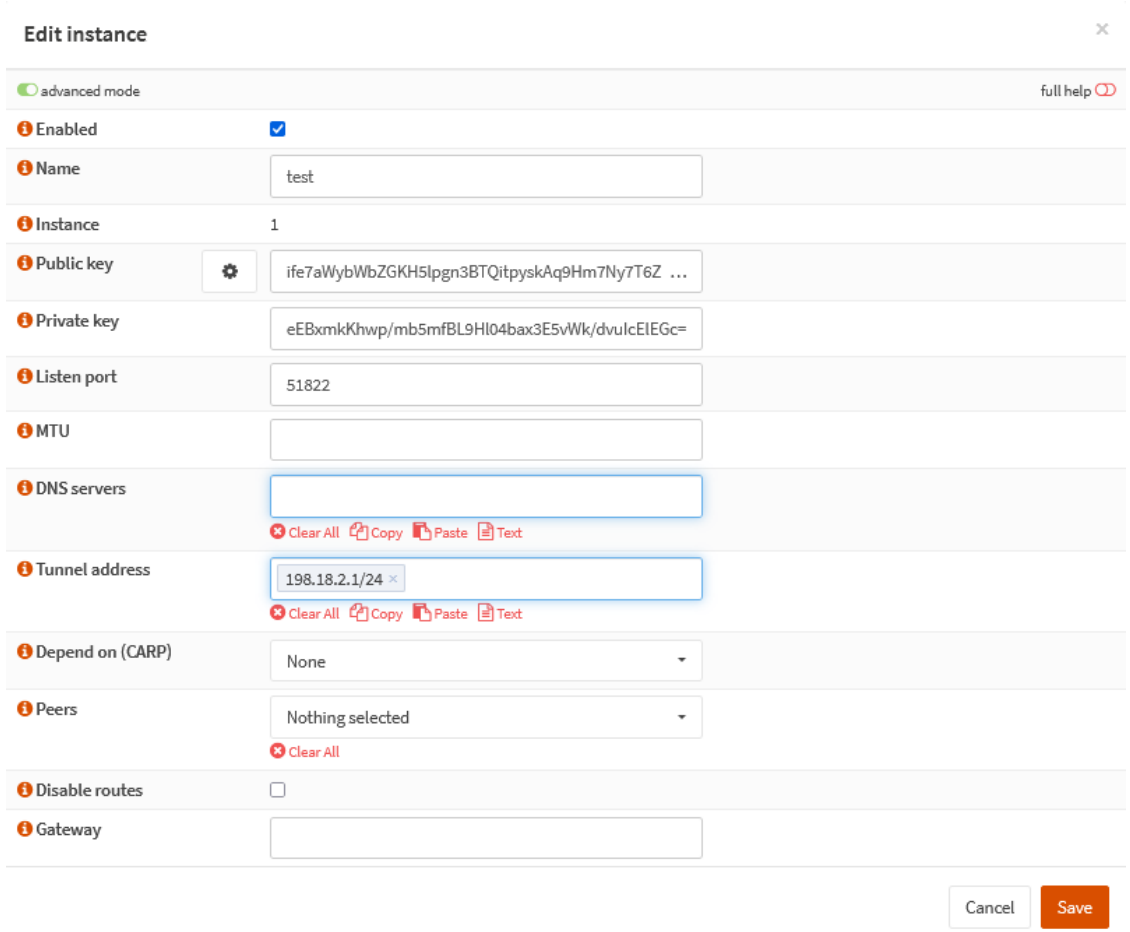


Einrichten eines neuen Labor-VPN

In OPNSense

1. Eine neue **Wireguard**-Instanz erstellen
2. Parameter einstellen
   - Schlüssel
   - UDP-Port
   - Tunnel-Adresse (internes VPN-Subnet)
3. Interface erstellen und zuweisen
4. Firewallregeln erstellen
5. Clients erstellen (Peers)
   - 1 Labor-Router, mit Route ins Labor-LAN
   - N Clients für Remote-Zugriff

Konflikte bei Port, VPN-Subnet und Labor-LAN vermeiden!

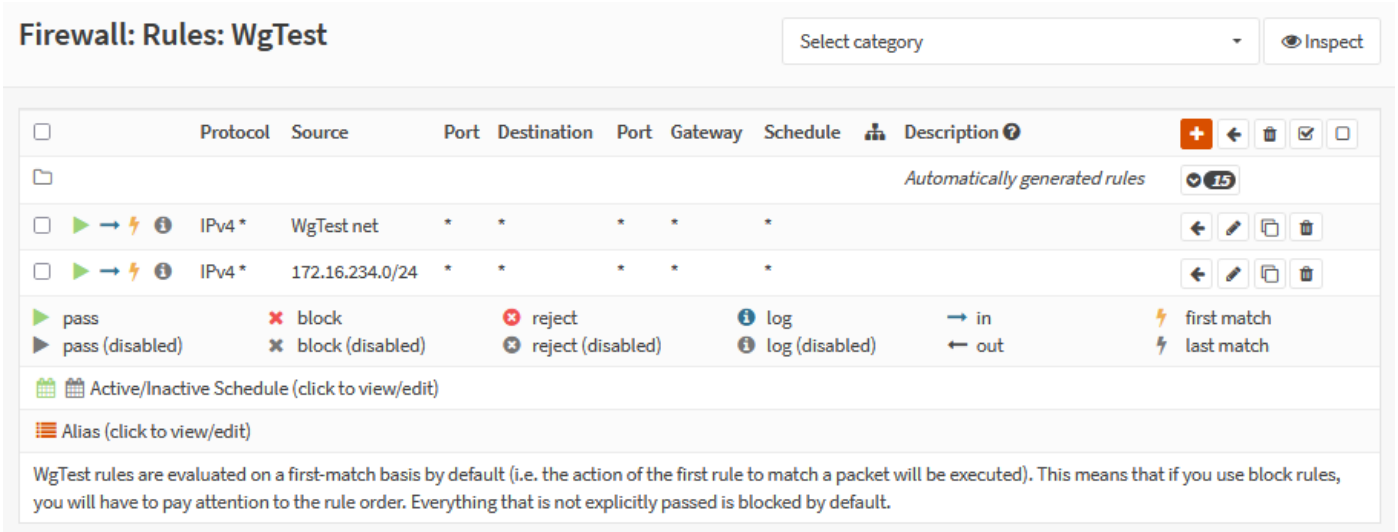


Firewallregeln

VPNs sollen gegeneinander isoliert werden

Quellen
- VPN-Subnet
- Labor-LAN

Ziele
- ANY (Internetzugriff)
- Labor-LAN (oben enthalten)

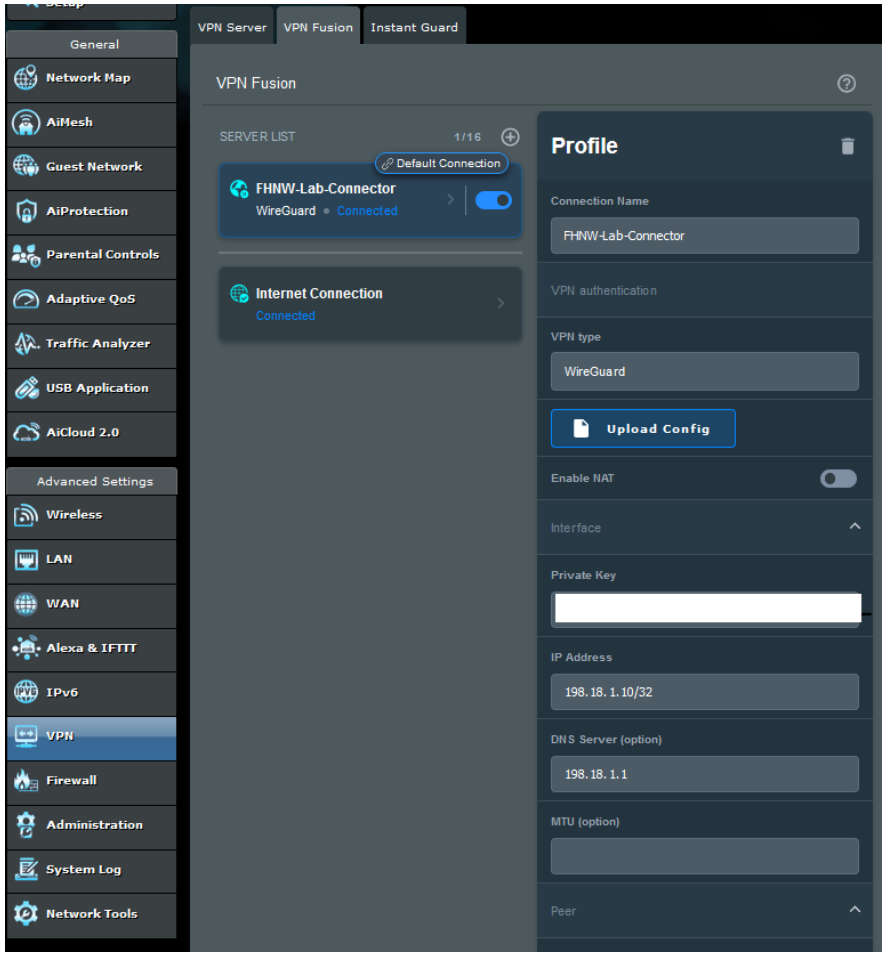


Lab Connector – Labor-Router

Jeder Router möglich, der **Wireguard** als **Client** unterstützt

ASUS RT-AX58U

- Wireguard Client out of the box (VPN Fusion)
- kann gesamten Traffic durch VPN leiten
- Auch für site-to-site geeignet

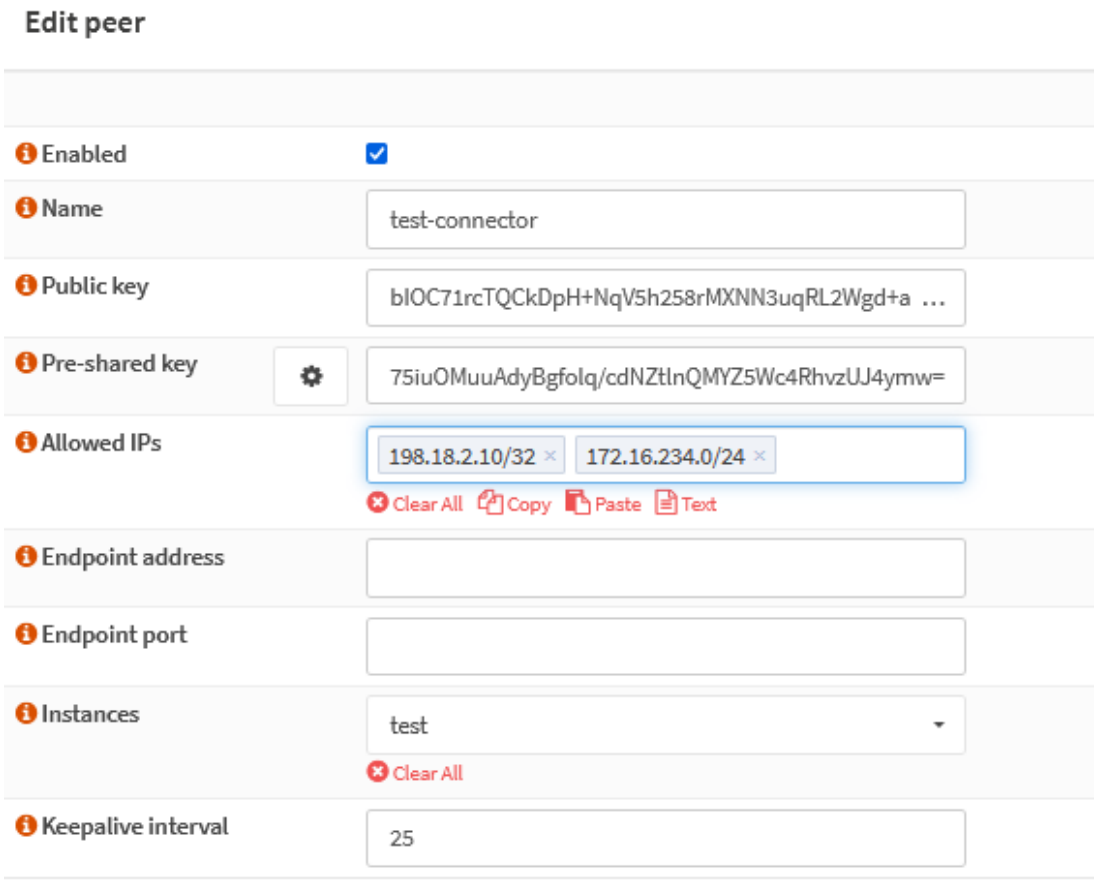


VPN Client für Labor-Router konfigurieren

In OPNSense Peer konfigurieren
- Schlüssel
- Bei AllowedIPs muss Labor-LAN ergänzt werden
  → wird über diesen Peer geroutet

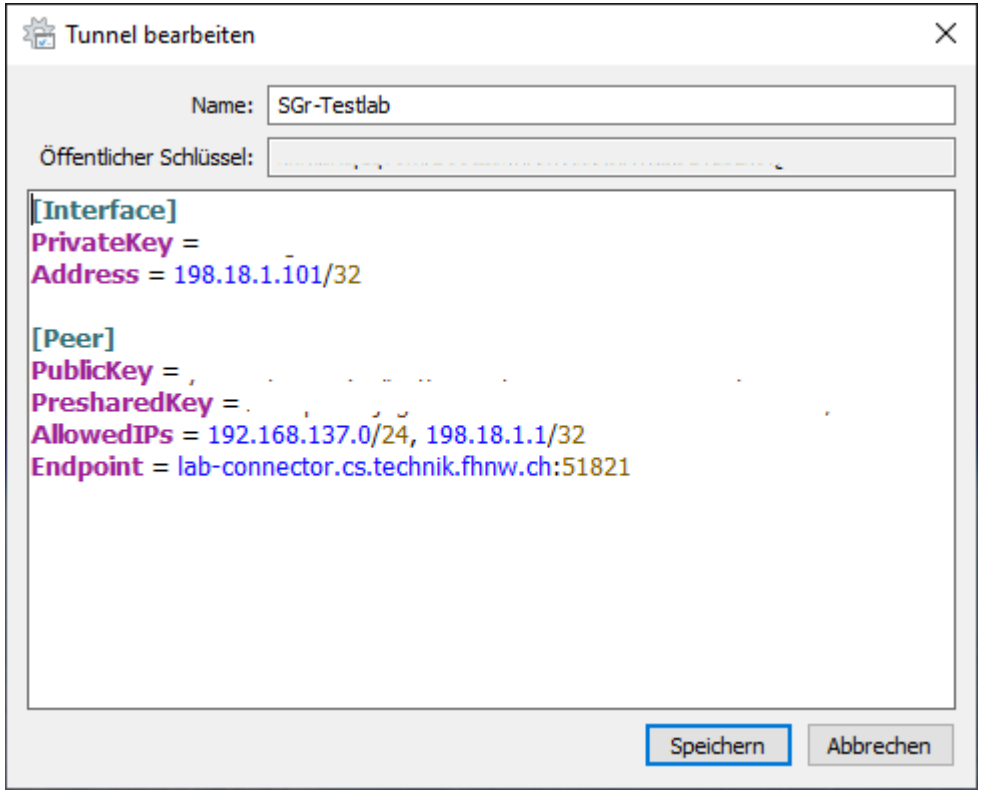
Labor-LAN kann immer nur über 1 Peer geroutet werden!

Auf dem Router
- Endpoint
- Schlüssel
- Bei AllowedIPs 0.0.0.0/0 eintragen → gesamten Traffic via VPN routen



VPN Client für Remote-Zugriff konfigurieren

- Endpoint (VPN Gateway)
- Public + Private Keys
- VPN-Adresse – i.d.R. fix pro Client
- AllowedIPs bestimmt die Routen des Clients
  - Labor-LAN
  - VPN-Adresse des Gateway (optionaler DNS)



Zusammenfassung – Ablauf

1. Vorabklärung
   – Adressierung (Labor-LAN)
2. Passenden Router organisieren
3. Labor-VPN einrichten lassen
4. Router von Corporate IT freischalten lassen (MAC-Adresse, 1 Zugriffsregel für VPN-Tunnel)
5. Router konfigurieren
6. Remote-Clients einrichten

Ausblick

Zukünftige Erweiterung auf IPv6

Sonstige Ideen für Verbesserungen?